May 10, 2022

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Subject: Recommendations to Strengthen Cybersecurity in Healthcare

Dear Mr. Secretary:

The National Committee on Vital and Health Statistics (NCVHS) serves as your advisory body on health data, statistics, privacy, confidentiality, information security, and national health information policy. NCVHS is charged with studying and identifying "privacy, confidentiality and information security measures to protect individually identifiable health information."[1] This letter makes recommendations on ways to enhance the security of U.S. healthcare entities to protect the safety of patients and the reliability of lifesaving technologies in the face of a sophisticated and rapidly evolving threat landscape.

In response to the rising number of cybersecurity incidents affecting the healthcare industry, NCVHS held a hearing on July 14, 2021, to better understand the cybersecurity landscape and to explore how best to protect information and patients. Motivated by news of escalating cybersecurity risks (e.g., ransomware,[2] denial of service attacks,[3] and phishing[4]), studies showing that cyber-attacks have real consequences on patient safety,[5] and a high-profile lawsuit claiming the first loss of life in the U.S. attributable to a cyber-attack,[6] the Committee sought to understand the challenges faced by a wide

[1] Charter, National Committee on Vital and Health Statistics, para. H. (Jan. 21, 2022): https://ncvhs.hhs.gov/about/charter/

[2] See, for example, Tonya Riley, "Cybersecurity 202: DHS Chief wants to fight another epidemic — hackers holding data hostage," *Washington Post* (Feb. 26, 2021). https://www.washingtonpost.com/politics/2021/02/26/cybersecurity-202-dhs-chief-wants-fight-another-epidemic-hackers-holding-data-hostage/ (visited Apr. 11, 2022).

[3] See, for example, Jessica Davis, "Denial-of-service attacks on healthcare poised to explode," *Healthcare IT News* (May 16, 2017). https://www.healthcareitnews.com/news/denial-service-attacks-healthcare-poised-explode (visited Apr. 11, 2022).

[4] See, for example, Jessica Davis, "Phishing Attack on Five Rivers Health Impacts 156k Patients," *Health IT Security* (June 11, 2021). https://healthitsecurity.com/news/phishing-attack-on-five-rivers-health-impacts-data-of-156k-patients (visited Apr. 11, 2022).

[5] Ponemon Institute, "The Impact of Ransomware on Healthcare During COVID-19 and Beyond," *Censinet* (Sept. 2021). https://www.censinet.com/ponemon-report-covid-impact-ransomware (visited Apr. 11, 2022) (finding that when hospitals experience ransomware events, length of patient stay increases, which can lead to exposure to other illnesses or complications, delays in procedures and lab tests, and unfavorable outcomes).

[6] Joseph Marks, "Ransomware attack might have caused another death," *Washington Post* (Oct. 1, 2021). https://www.washingtonpost.com/politics/2021/10/01/ransomware-attack-might-have-caused-another-death/ (visited Apr. 11, 2022) (reporting that a ransomware attack against an Alabama hospital may have led to a baby's

variety of parties in the healthcare domain, e.g., government, public health, small rural hospitals, and large integrated healthcare systems. The Committee also sought to understand the scope and breadth of security risks, and how best to address those challenges in protecting the safety of patients and the healthcare system itself. Security experts representing healthcare providers, insurers, academics, and all levels of government provided testimony.

NCVHS considers privacy and information security a vital part of the wellbeing of the nation. To best protect our population, healthcare entities of all types and sizes must be able to combat the increasing threat of cyber-attacks while taxed with responding to a global pandemic. Failure to manage these threats appropriately and promptly could result in serious harm to patients. Privacy and information security practices must be strong, but also nimble enough to protect against a rapidly diversifying threat landscape. NCVHS recommends the following actions HHS should take to help healthcare entities enhance information security. These recommendations are based on careful consideration of the expert testimony obtained during the July 2021 hearing, news, industry statements, and the personal expertise of Committee members.

We believe that four critical actions, spelled out below, will encourage healthcare entities to secure their environments and support them as they undertake that challenge.

Specifically, NCVHS recommends that HHS:

1. **Strengthen the HIPAA Security Rule by:**
   - **A. Eliminating from the addressable implementation specifications the choice to not implement a specification or alternative, and instead requiring covered entities to implement the specification in the Rule or to adopt a documented reasonable alternative.**
   - **B. Including additional minimum cybersecurity hygiene requirements.**

2. **Mandate basic cybersecurity requirements for any organization that is a recipient of federal funds, in partnership with other appropriate government agencies.**

3. **Further enhance communication and education regarding the HIPAA Security Rule and security threats and incidents by:**
   - **A. Providing more robust guidance regarding enterprise-wide risk analysis and risk mitigation requirements to ensure covered entities and business associates understand the full breadth of the Security Rule's expectations and requirements.**
   - **B. Facilitating, with other appropriate government agencies, more coordination and collaboration among public and private sector parties during incidents, including work to coordinate the identification of threats to critical infrastructure.**
   - **C. Leveraging, in partnership with other appropriate government agencies, the Office for Civil Rights (OCR) cybersecurity newsletters as real-time playbooks on common cybersecurity incidents.**

---

death in 2019 because an electronic display of fetal heart rate was unavailable to the nursing staff); *See also* William Ralston, "The untold story of a cyberattack, a hospital and a dying woman," *Wired* (Nov. 11, 2020). https://www.wired.co.uk/article/ransomware-hospital-death-germany/ (visited Apr. 11, 2022) (describing death of a patient in Germany who had to be re-routed to a new hospital after original destination experienced a cyber-attack).

D. Encouraging entities to undergo the free CISA Cyber Hygiene Services to reduce exposure to cyber threats.

4. Evaluate, in concert with other appropriate government agencies, the level of compliance with the HIPAA Security Rule and provide assistance to healthcare entities with the greatest need in meeting the enhanced minimum security requirements.

Attached please find an Appendix with detailed justifications for each of the Committee's recommendations.

According to at least one published report, for the past 11 years, the cost of data breaches in the health sector has been notably higher than in all other industries, and the cost increased (on average) from $7.13 million in 2020 to $9.23 million in 2021.[7] In 2017, the Health Care Industry Cybersecurity Task Force, established by HHS, reported to Congress that healthcare cybersecurity was in critical condition and made recommendations designed to ensure the US healthcare system could deliver effective and safe care in the face of cybersecurity threats. To date, many of the recommendations made by the Task Force still require action as the industry struggles to keep up with a rapidly changing environment of new technologies, old equipment, and vexingly creative and aggressive threat actors, exacerbated by the pandemic.[8] The increasingly perilous cyber threat landscape has resulted in expensive data breaches, delays, or denials of patient care, and even the loss of patient life. Stress on the nation's critical infrastructure due to the pandemic further taxes the healthcare ecosystem. NCVHS urges prompt consideration and implementation of our recommendations to protect the safety and health of all Americans.

Sincerely,

/s/

Jacki Monson, J.D., Chair
National Committee on Vital and Health Statistics

Attachment: Appendix—NCVHS Recommendations to Strengthen Cybersecurity in Healthcare

[7] IBM Security, "Cost of a Data Breach Report 2021," at 15 (July 2021). https://www.ibm.com/security/data-breach (visited Apr. 11, 2022).
[8] Health Care Industry Cybersecurity Task Force, "Report on Improving Cybersecurity in the Health Care Industry" Office of the Assistant Secretary for Preparedness & Response (June 2017). https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf (visited Apr. 11, 2022).

APPENDIX
NCVHS Recommendations to Strengthen Cybersecurity in Healthcare

Recommendation 1: Strengthen the HIPAA Security Rule by:

A. Eliminating from the addressable implementation specifications the choice to not implement a specification or alternative, and instead requiring covered entities to implement the specification in the Rule or to adopt a documented reasonable alternative.

The Committee recommends that HHS eliminate the ability of a covered entity or business associate to avoid adopting any solution under the HIPAA Security Rule's "addressable" (recommended but voluntary) implementation specifications. Rather, covered entities and business associates should be required either to be in full compliance or to adopt a reasonable documented alternative.

Despite efforts on the part of practitioners in the field, voluntary efforts, and actions of the government, healthcare entities have come short of success in bridging the gaps between what is needed to secure patient information and medical devices and the realities of today's cybersecurity landscape. A recent College of Healthcare Information Management Executives (CHIME) survey of acute and ambulatory care organizations found that just 32% of those organizations have a comprehensive security program, and only 26% of long-term and post-acute care facilities met the minimum security requirements.[9] The survey also found that healthcare organizations are more likely to adopt technology-focused security measures and neglect the people and process measures necessary for a comprehensive security program. They continue to deprioritize incident recovery plans, fail to leverage "purple teaming,"[10] and opt out of social engineering risk assessments because they are not mandated.

These studies and reports are just a few examples demonstrating that voluntary (or addressable) industry practices are inadequate to ensure our healthcare infrastructure is properly protected, but the Security Rule continues to permit covered entities to avoid what are now reasonable, minimum requirements. In its 2013 guidance describing the difference between required and addressable implementation specifications, OCR stated that "a covered entity must implement an addressable implementation specification if it is reasonable and appropriate to do so, and must implement an equivalent alternative if the addressable implementation specification is unreasonable and inappropriate, and there is a reasonable and appropriate alternative." [11] However, the guidance permits a covered entity or business associate to "not implement either an addressable implementation specification or an alternative."

---

[9] Jill McKeon, "32% of Healthcare Organizations Have a Comprehensive Security Program," *Health IT Security* (Nov. 22, 2021). https://healthitsecurity.com/news/32-of-healthcare-organizations-have-a-comprehensive-security-program (visited Apr. 11, 2022).

[10] Purple teaming refers to exercises that both simulate and test vulnerabilities, known as "red teaming," and practice defending against their exploitation, known as "blue teaming." Jon Boyens, et al. "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," *Nat'l Inst. Of Standards & Tech*., Spec. Publ. 800-161, Appx F, at F-6 (Apr. 2015). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf (visited Apr. 11, 2022).

[11] *See* Office for Civil Rights, U.S. Dept of Health and Human Services (OCR), "What is the difference between addressable and required implementation specifications in the Security Rule?" (July 26, 2013). https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html.

The Committee concludes that covered entities and business associates should not be given an option to not implement the provisions of the HIPAA Security Rule but should be required to adopt the basic building blocks of good security hygiene, or a documented, reasonable alternative. The Committee recognizes that some flexibility in exactly how security measures are adopted is appropriate and desirable. Therefore, we recommend that an entity document how they considered the requirement and adopted a reasonable alternative if unable to adopt the implementation specifications as described by the Security Rule.

B. Including additional minimum cybersecurity hygiene requirements.

NCVHS recommends that the HIPAA Security Rule be enhanced to include additional minimum cyber hygiene requirements that could prevent a cyber-attack or minimize the impact should one occur. In 2013, the Security Rule was enhanced to bring business associates under the direct enforcement authority of OCR,[12] but the substance of the Security Rule has not changed in 20 years, while the security landscape has changed significantly. Security controls that were once very expensive and only reasonable for large companies to implement are now commonplace, appropriate, and affordable for small and medium-sized organizations. Moreover, the availability of legal, organizational, and technical consulting services is more widespread and accessible.

Most cyber-attacks are successful due to lack of basic security controls. Hospitals or other health care providers who fail to adopt the basic security controls recommended in this letter have been subject to ransom attacks resulting in a variety of calamitous circumstances, for example, the need to shut down the entire information technology structure to further prevent the threat actors from taking patient information;[13] the diverting of patients to other hospitals;[14] or the delay of medical procedures.[15] Basic cybersecurity hygiene can prevent issues and help to lessen their impacts when they do occur.

NCVHS recommends that HHS consider enhancing the Security Rule to include the following new requirements: (1) designation of a qualified information security official, (2) elimination of default passwords, (3) adoption of multi-factor authentication, (4) institution of offline backups, (5) installation of critical patches within a reasonable time, and (6) transparency of impact and vulnerability

---

[12] Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.

[13] Sonoma Valley Hospital Press Release, "Hospital Well On The Way To Restoring Systems Following Cyberattack" (Nov. 11, 2020). https://www.sonomavalleyhospital.org/hospital-well-on-the-way-to-restoring-systems-following-cyberattack/; see also Anne Ward Ernst, "Sonoma Valley Hospital's 'security incident' was Russian ransomware attack," *Sonoma Index-Tribune* (Oct 30, 2020). https://www.sonomanews.com/article/industrynews/sonoma-hospitals-security-incident-was-russian-ransomware-attack/.

[14] Shari Rudavsky, "Eskenazi Health remains on diversion days after ransomware attack," *Indianapolis Star* (Aug. 9, 2021). https://www.indystar.com/story/news/health/2021/08/09/eskenazi-health-still-diversion-days-after-ransomware-attack/5546251001/ (visited Apr. 11, 2022).

[15] Greater Baltimore Medical Center Press Release, "Computer Networking Incident Update (Jan 6, 2020). https://www.gbmc.org/computer-network-incident-update-12-06-2020; see also Hallie Miller, "GBMC Health Care restoring electronic medical records after ransomware incident" *Baltimore Sun* (Jan. 7, 2021). https://www.baltimoresun.com/health/bs-bz-gbmc-ransomware-baltimore-20210107-prjyry7hffhn3lyzs4qpsfcxy4-story.html (visited Apr. 11, 2022).

disclosures.[16] The required standards should be more reflective of modern industry best practices. When NCVHS approved the substance of this letter, we anticipated that OCR would issue a Request for Information about the Security Rule.[17] Since then, OCR published "Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended,"[18] the responses to which may make strides toward achieving this recommendation. We are also aware that the Department has heard from industry representatives that they are anxious to see implementation of Public Law 116-321, which would give covered entities regulatory relief for following industry standard best practices.[19]

(1) Qualified information security official

The Security Rule should require the designation of a *qualified* information security official responsible for the development and implementation of policy and procedures. Currently, HIPAA merely requires the identification of an official responsible for the development and implementation of security policies and procedures.[20] While this is a nuanced difference, the emphasis on qualifications would ensure those responsible for information security have the necessary education and skills to do so. In a 2020 report, IBM reported that of 524 companies surveyed, only 27% of respondents said that the Chief Information Security Officer was most responsible for cybersecurity policy and technology decision-making.[21] This problem is likely to be more acute at healthcare organizations where patient care is more highly valued than cybersecurity.[22] For smaller organizations, a qualified official might be a shared resource among many small entities. Such smaller organizations often have limited access to trained security professionals and cybersecurity resources due to financial constraints.[23]

(2) Elimination of default passwords or hardcode passwords

---

[16] See Pub. L. 116-321, 134 Stat. 5072, (amending the Health Information Technology for Economic and Clinical Health Act to require the Secretary to consider certain recognized security practices of covered entities and business associates when making certain determinations).

[17] U.S. General Services Administration and Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, *Unified Agenda and Regulatory Plan*, Fall 2021, OCR, "HIPAA Rules: Request for Information on Sharing Civil Money Penalties or Monetary Settlements with Harmed Individuals, and Recognized Security Practices Under HITECH," https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=0945-AA04 (visited May 3, 2022).

[18] Office for Civil Rights, HHS, Request for Information, 87 Fed. Reg. 19833-39 (Apr. 6, 2022), *available at https*://www.federalregister.gov/documents/2022/04/06/2022-07210/considerations-for-implementing-the-health-information-technology-for-economic-and-clinical-health *(visited May 3, 2022).*

[19] See Subcommittee on Privacy, Confidentiality, and Security, "Meeting Summary, Hearing on Security in Healthcare" 6-7, *National Committee on Vital and Health Statistics* (July 14, 2021). https://ncvhs.hhs.gov/wp-content/uploads/2021/11/2021-07-14-NCVHS-PCS-Hearing-Summary-FINAL-508.pdf (Notes on Decker testimony).

[20] Security Standards for the Protection of Electronic Protected Health Information ("HIPAA Security Rule"), 42 C.F.R. § 164.308(a)(2).

[21] IBM Security, "Cost of a Data Breach Report 2020," at 44 (July 2020). https://www.ibm.com/downloads/cas/RZAX14GX (visited Apr. 11, 2022).

[22] Jalali, Mohammad S, and Jessica P Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," *Journal of medical Internet research* vol. 20,5 (May 28, 2018). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/ (visited Apr. 11, 2022).

[23] Health Care Industry Cybersecurity Task Force, "Report on Improving Cybersecurity in the Health Care Industry" 35, 43 (June 2017). https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf (Report outlining recommendations to address the challenge of cyber-attacks targeting health care) (visited Apr. 11, 2022).

Among the standard best practices for which Public Law 16-321 would provide regulatory relief is the elimination of default and hardcoded passwords.[24] Cybercriminals look for the lowest common denominator when attacking a system. One of the lowest denominators they can find are the default passwords provided with built-it in accounts. This issue has been on security practitioners' radars for years, but no easy resolution has emerged. For example, in 2013, the Department of Homeland Security warned that 300 medical devices could be vulnerable to malicious hacking due to hardcoded default passwords.[25] In 2020, General Electronic Corporation made the news when publicly known usernames and passwords exposed healthcare imaging devices to hacking,[26] and just this year, more reports are showing that at least half of internet-connected devices in hospitals are vulnerable to hacks — with infusion pumps being the most at risk.[27]

Default user identification and default passwords are built into operating systems, databases, and software when initiated or shipped. These defaults are often the same for all copies of a particular software version and can carry high level system privileges. As such, when healthcare entities and business associates do not cease the use of default passwords and assign new ones upon installation, cybersecurity risk rapidly increases. This is because default passwords are not a secret — they can be found published on the internet, in vendor handbooks, and via other easy to access sources. However, tools and technologies to assist organizations in eliminating the use of default passwords are just as readily available. Therefore, the elimination of default passwords should be a minimum cyber hygiene requirement in the HIPAA Security Rule.

(3) Multi-factor authentication

Multi-factor authentication is a security procedure that requires individuals to provide more than one verification point to gain access to an electronic resource — for example, an online account or a virtual private network (VPN).[28] Multi-factor authentication is considered a core component of identity and access management. It is also considered a vital layer in securing healthcare networks and applications from cybercriminals. For example, a common response to healthcare data breaches is the adoption of multi-factor authentication as part of remediation efforts.[29] Resources requiring multi-factor

[24] Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security (CISA), "Bad Practices," https://www.cisa.gov/BadPractices.; "Cyber Hygiene Services," https://www.cisa.gov/cyber-hygiene-services; and "Known Exploited Vulnerabilities," https://cisa.gov/known-exploited-vulnerabilities (visited Apr. 11, 2022).
[25] Arezu Sarvestani, "Hacking: Password risk affects some 300 medical devices, says Homeland Security," *Mass Device* (July 5, 2013). https://www.massdevice.com/hacking-password-risk-affects-some-300-medical-devices-says-homeland-security/ (visited Apr. 11, 2022).
[26] Lucian Constantin, "Publicly known support credentials expose GE Healthcare imaging devices to hacking," *CSO Online* (Dec. 8, 2020). https://www.csoonline.com/article/3600164/publicly-known-support-credentials-expose-ge-healthcare-imaging-devices-to-hacking.html (visited Apr. 11, 2022).
[27] Nicole Wetsman, "Half of internet-connected devices in hospitals are vulnerable to hacks, report finds," *The Verge* (Jan. 19, 2022). https://www.theverge.com/2022/1/19/22891440/internet-connected-medical-devices-vulnerable (visited Apr. 11, 2022).
[28] Definition of "MFA," NIST Computer Security Resource Center Glossary (NIST Glossary). https://csrc.nist.gov/glossary/term/mfa (visited Apr. 11, 2022).
[29] *See* Marianne Kolbasuk McGee, "Clinic Notifies 212,500 About 2020 Breach Involving Fraud," *Government Information Security* (Jan. 4, 2022). https://www.govinfosecurity.com/clinic-notifies-212500-about-2020-breach-involving-fraud-a-18238 (visited Apr. 11, 2022) (describing the response of a Florida-based gastroenterology practice working to remediate the impacts of a data breach, including implementing multi-factor authentication throughout its IT systems).

authentication for access are less vulnerable to brute force attacks[30] because they require users to input at least two types of information specific to that individual (for example, something they *know* — a password or pin number; something they *have* — a badge or smartphone; or something they *are* — a fingerprint, face scan, or voice print). Additionally, because there are multiple data points required before access can be granted, cybercriminals require significantly more resources to attempt an attack — something that often makes a target less appealing.

(4) Offline backups

Offline backups allow healthcare entities and business associates a myriad of benefits. Offline backups are less prone to cybersecurity threats, easier to monitor, and easier to recover. They also help organizations, no matter their size, protect access to their data. Offline backups are also helpful if an organization should experience a ransomware attack in which their records are encrypted by a cybercriminal, since it can more easily restore its network or use the copy to recover the data. This reduces costs and risks to patients.

For example, consider the case of the cybersecurity issues faced by Sonoma Valley Hospital which suffered a ransomware cyberattack on October 11, 2020, resulting in the hospital shutting down the entire information technology structure in an attempt to prevent the threat actors from taking patient information.[31] The hospital later notified patients that it believed some patient data was compromised, such as patient name, address, birthdate, insurer group number and subscriber number, as well as diagnosis or procedure codes, date of service, place of service, amount of claim, and secondary payer information.[32] Compare Sonoma Valley's experience with a similar situation at the Ottawa Hospital in 2016. Similarly faced with a ransomware attack due to a phishing campaign, Ottawa's information technology administrators were able to clean the drives and reimage their data with recent backups that were available and ready to go.[33] Had Sonoma hospital had an offline backup, it could have prevented the need to shut down power to the information technology systems. This basic cybersecurity hygiene practice can prevent issues and help to lessen their impacts when they do occur.

(5) Installation of critical patches and addressing known vulnerabilities within a reasonable timeframe.

Patching and updating systems is one of the most important information security practices an organization can implement. [34] Patches and updates are fixes to the software code to address

---

[30] A brute force attack, for the purposes of this letter, is a type of hacking that uses trial and error to guess possible passwords, login credentials, or encryption keys. "Brute Force Password Attack," *NIST Glossary*. https://csrc.nist.gov/glossary/term/brute_force_password_attack(visited Apr. 11, 2022).

[31] Sonoma Valley Hospital Press Release, "Sonoma Valley Hospital Notifies Patients Affected By Ransomware Attack," (Dec. 10, 2020). https://www.sonomavalleyhospital.org/sonoma-valley-hospital-notifies-patients-affected-by-ransomware-attack/ (visited Apr. 11, 2022).

[32] Anne Ward Ernst, "67,000 hospital patients notified about data breach," *Sonoma Index-Tribune* (Dec. 14, 2020). https://www.sonomanews.com/article/news/67000-hospital-patients-notified-about-data-breach/ (visited Apr. 11, 2022).

[33] Chris Sienko, "Ransomware Case Studies: Hollywood Presbyterian & The Ottawa Hospital" *Infosec* (June 17, 2016). https://resources.infosecinstitute.com/topic/ransomware-case-studies-hollywood-presbyterian-the-ottawa-hospital/ (visited Apr. 11, 2022).

[34] CISA, "Reducing the Significant Risk of Known Exploited Vulnerabilities," https://www.cisa.gov/known-exploited-vulnerabilities (visited Apr. 11, 2022).

vulnerabilities that would otherwise allow a cybercriminal to access or even take over an organization's network, compromising systems and the data they store. In a healthcare context, failing to patch a known, critical vulnerability could allow a cybercriminal to take over a hospital network. Without access to the network, caregivers could lose the ability to run vital tests, be forced to transfer patients to other locations delaying treatment, or even face the need to cancel lifesaving surgeries. Patching issues are well known. In a 2019 report that specifically looked at vulnerability and patch management, researchers found that 48 percent of respondents experienced one or more data breaches in the prior two years, and 60 percent said that those breaches could have occurred because a patch was available for a known vulnerability but not applied.[35] Of these respondents, 62 percent were unaware that their organizations were at risk before the breach.[36]

Consider the discovery of a seven-year breach of Florida Medicaid applicants' protected health information and the exposure of 3.5 million records in 2020 by the Florida Healthy Kids Corporation. The breach was caused by the failure of a business associate to properly patch vulnerabilities from 2013 to 2020, resulting in one of the largest healthcare data breaches in history.[37] The 2017 WannaCry ransomware incident is another example of the significant consequences to healthcare systems when systems are not properly patched.[38]

Requiring the installation of critical patches within a reasonable timeframe would lessen the risks described above. A reasonableness criterion would also allow for organizations to feel confident that they have the time to test patches and updates to ensure they can be safely deployed, while also placing an urgency on conducting those tests and deploying the patches. Additionally, appropriate management of patching and updates helps organizations ensure they are following other basic cyber hygiene requirements such as knowing what is connected to and running on their networks, implementing security settings, and limiting users with administrative privileges.

(6) Transparency of impact and vulnerability disclosures.

When security researchers discover a vulnerability, transparency in the impact of those vulnerabilities, the release of those vulnerabilities, and information about how to timely correct them should be transmitted to healthcare entities. Doing so helps to ensure real or potential security threats can be quickly accounted for in the healthcare environment before those vulnerabilities are exploited by cybercriminals. While government agencies may share vulnerability disclosures with the Cybersecurity and Infrastructure Security Agency (CISA), there should be more effort to require that they share those vulnerabilities quickly, so the information can be used by critical sectors like healthcare. Also, healthcare entities and business associates should have a straightforward path to be able to share the same information without fear of retribution.

---

[35] Ponemon Institute, "COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE," at 5 *ServiceNow* (2019). https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf (visited Apr. 11, 2022).

[36] *Id.*

[37] Steve Alder, "Failure to Patch Results in 7-Year Breach of Florida Medicaid Applicants' PHI and Exposure of 3.5 Million Records," *HIPAA Journal* (Feb. 1, 2021). https://www.hipaajournal.com/failure-to-patch-results-in-7-year-breach-of-florida-medicaid-applicants-phi/ (visited Apr. 11, 2022).

[38] Danny Palmer, "WannaCry ransomware: Hospitals were warned to patch systems to protect against cyber-attack – but didn't," *ZDNet* (Oct. 27, 2017). https://www.zdnet.com/article/wannacry-ransomware-hospitals-were-warned-to-patch-system-to-protect-against-cyber-attack-but-didnt/(visited Apr. 11, 2022).

To assist organizations in reducing their exposure to threats and support a proactive approach to mitigating attack vectors, CISA offers several scanning and testing services. These include vulnerability scanning, web application scanning, phishing campaign assessment, and remote penetration testing.[39]

Recommendation 2: **Mandate basic cybersecurity requirements for any organization that is a recipient of federal funds, in partnership with other appropriate government agencies.**

Healthcare entities frequently are provided with federal funds to assist with various efforts or as payment for certain types of patients. NCVHS believes that using federal leverage to encourage compliance would be a powerful incentive to get entities to improve their cybersecurity posture. Therefore, we recommend that federal funds should be contingent on the implementation of minimum cybersecurity hygiene requirements or compliance with the enhanced HIPAA Security Rule in Recommendation 1.

These requirements can be technology neutral and should be capable of being implemented by any type or size of organization. For example, minimum hygiene requirements could be as simple as noted best practices for cybersecurity, such as:

1) having a formal, well documented cybersecurity program;
2) conducting annual enterprise-wide risk assessments;
3) defining and assigning information security roles and responsibilities;
4) having strong access control processes and procedures;
5) conducting cybersecurity awareness training;
6) having an effective business resiliency program (tested annually) that addresses business continuity, disaster recovery, and incident response; and
7) maintaining timely patching and updates for software.

Implementing basic cybersecurity hygiene does not have to be onerous, since there are many ways to meet these best practices. However, conditioning federal funds on the development and maintenance of basic cybersecurity hygiene will go a long way to better protect the privacy and security of US residents as well as the ability of US industries to maintain basic operations in a high-risk cybersecurity landscape. To that end, CISA makes available to critical infrastructure organizations, at no charge, scanning, assessment, and testing services mentioned in Recommendation 1.B.(6) above.[40] Organizations that do not meet the "critical infrastructure" criterion can still avail themselves of the examples and advice on CISA's website.

[39] CISA, "Cyber Hygiene Services," https://www.cisa.gov/cyber-hygiene-services (visited Apr. 11, 2022).
[40] *Id.*

<u>Recommendation 3</u>: Further enhance communication and education regarding the HIPAA Security Rule and security threats and incidents by:

A. Providing more robust guidance regarding enterprise-wide risk analysis and risk mitigation requirements to ensure covered entities and business associates understand the full breadth of the Security Rule's expectations and requirements.

OCR has provided multiple tools and guidance on risk analysis.[41] However, despite the existence of these resources, one of the most common findings in resolution agreements issued by OCR is that the organization failed to perform an adequate enterprise-wide risk analysis.[42] During the July hearing, one presenter discussed issues with risk analyses seen in OCR audit findings from 2016 to 2017. In those audits, OCR determined only 14% of covered entities and 17% of business associates were compliant with the risk analysis requirements of HIPAA.[43]

HIPAA requires a risk analysis to be an accurate and thorough enterprise-wide assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.[44] In the OCR audit findings, both covered entities and business associates failed to comply with the existing regulations, leading to the conclusion that what constitutes an accurate and thorough enterprise-wide assessment is not clear or is being interpreted by regulated entities differently than by OCR. Often, OCR finds inadequate risk analysis after a cyber security incident.

We recognize that some small organizations will not have the resources to conduct complex risk analysis. Should OCR raise the floor for HIPAA Security Rule compliance (Recommendation 1), and provide updated, more detailed guidance on risk analysis, healthcare organizations and their business associates may be better able to meet expectations regarding compliance with risk assessment. This updated guidance should include best practices for conducting risk analyses and outline the expectations of OCR more clearly.

In the guidance, we recommend OCR emphasize conducting an enterprise-wide risk analysis that considers all devices connecting to the network. While OCR focused on the electronic health record in its 2013 guidance,[45] the EHR is no longer the only risky access point. The myriad of mobile devices together with the "internet of things" also puts healthcare organizations at risk.

---

[41] OCR, "Guidance on Risk Analysis," U.S. Dept. of Health & Human Services (July 22, 2019). https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (OCR Risk Guidance).

[42] OCR, "Resolution Agreements: Resolution Agreements and Civil Money Penalties," (Mar. 28, 2022). https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html. On this page, one can review OCR agreements with parties that have findings against them. Sampling the documents shows that failure to perform an enterprise-wide risk analysis is a frequent finding.

[43] Subcommittee on Privacy, Confidentiality, and Security, "Meeting Summary, Hearing on Security in Healthcare" at 14, *National Committee on Vital and Health Statistics* (July 14, 2021),\. https://ncvhs.hhs.gov/wp-content/uploads/2021/11/2021-07-14-NCVHS-PCS-Hearing-Summary-FINAL-508.pdf (Notes on Noonan testimony: "OCR's 2016-2017 audit of HIPAA regulated entities found that most covered entities (86%) and business associates (83%) did not have a substantially compliant risk analysis.").

[44] HIPAA Security Rule, 42 C.F.R. § 164.308(a)(1)(ii)(A).

[45] OCR Risk Guidance, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

B. Facilitating, with other appropriate government agencies, more coordination and collaboration among public and private sector parties during incidents, including work to coordinate the identification of threats to critical infrastructure.

Healthcare entities are focused, above all else, on patient safety and care. Their mission is to provide for their communities. Unfortunately, threat actors are aware of this and take advantage of the position of healthcare entities who must respond to medical emergencies while protecting their systems, tasks that not only compete for resources, but also require rapid risk decisions based on limited information. Healthcare, like many industries, operates in a complex environment where each entity may be managing multiple incompatible technical systems with expensive aging components, multiple sub-level organizations, and a web of cross-industry relationships. This means information security teams are often faced with a threat environment larger or more complex than they can manage on their own. However, cybersecurity threat actors are generally industry agnostic and cast wide nets as they seek to obtain private information or disrupt operations to achieve financial gain. To help healthcare entities of all types and sizes combat cybersecurity risks, improved collaboration between the public and private sectors, especially during incidents, will help protect patients and provide avenues for information sharing that can lead to quick identification, containment, eradication, and remediation of cybersecurity threats.

Efforts by CISA, the Healthcare Coordinating Council, and the Health Information Sharing and Analysis Center are helping to create stronger partnerships and information sharing between the public and private sectors regarding cybersecurity threats. In particular, NCVHS applauds efforts to launch a new website for HHS's 405(d) Aligning Health Care Industry Security Approaches program.[46] However, these efforts need more coordination and support from the federal government, especially when it comes to healthcare. HHS can help advance those efforts by acting as a conduit for information, especially during active incidents, by using its communication and financial resources, and its ability to persuade other agencies and industries to protect the privacy and security of citizens. These efforts could include the establishment of a multi-agency alert center, coordination of multidisciplinary meetings, and the establishment of a security operations center where multiple sectors could feed or pull information.

HHS can also better reinforce these efforts by assisting with staffing and support. Many organizations working to better connect public and private organizations to advance cybersecurity in healthcare are made up of volunteers joined by a few federal officials. Providing more financial and staffing support would mean efforts can be more coordinated, focused, and productive. During the hearing, we heard that, of the various workgroups in the healthcare sector, only one has fulltime and contractor support from HHS – Health Sector Coordinating Council Cybersecurity Working Group.[47] Providing more resources to these efforts would help buttress work already being done and push forward new efforts more rapidly.

---

[46] OCR, "HHS launches website for the 405(d) Aligning Health Care Industry Security Approaches Program," (Dec. 1, 2021). https://www.hhs.gov/about/news/2021/12/01/hhs-launches-website-405d-aligning-health-care-industry-security-approaches-program.html; 405(d) Program, "HHS 405(d) Aligning Health Care Industry Security Approaches"; HHS Office of Information Security, https://405d.hhs.gov/public/navigation/home (visited Apr. 11, 2022).

[47] Subcommittee on Privacy, Confidentiality, and Security, "Meeting Summary, Hearing on Security in Healthcare," 6-7, *National Committee on Vital and Health Statistics* (July 14, 2021). https://ncvhs.hhs.gov/wp-content/uploads/2021/11/2021-07-14-NCVHS-PCS-Hearing-Summary-FINAL-508.pdf (Notes on Decker testimony).

C. Leveraging, in partnership with other appropriate government agencies, the Office for Civil Rights (OCR) cybersecurity newsletters as real-time playbooks on common cybersecurity incidents.

Our July 2021 hearing revealed that many healthcare entities, especially smaller and rural entities, lack large information security staffs that can identify and mitigate the multitude of cybersecurity risks to their organizations.[48] These entities also often lack the funding to contract with third parties to ensure their cybersecurity safety nets are able to detect, contain, eradicate, and recover from the wide variety of attacks present in the current threat landscape. Add to this, the increasing costs of cyber insurance, and many organizations feel trapped and resigned to the idea that a major breach is inevitable instead of preventable. A few government agencies are sending alerts to these organizations; however, the alerts are delayed and do not arrive when the threat is imminent.

HHS should convert OCR newsletters into playbooks on cyber-attacks and immediate real-time strategies to mitigate or even prevent cyber-attacks in partnership with other federal and state agencies. Such playbooks would help smaller organizations learn from the experience of larger ones both in the public and private sectors. They should outline best practices and continually be updated to ensure new threat intelligence is synthesized.[49] The work could be part of the increased collaboration in Recommendation 3.B. and would serve as a strong complement to the Security Risk Assessment tool developed by the Office of the National Coordinator for Health Information Technology in collaboration with OCR for medium and small providers. This approach would support real-time information sharing and assistance with incident containment and remediation.

D. Encouraging entities to undergo the free CISA Cyber Hygiene Services to reduce exposure to cyber threats.

As mentioned above in Recommendation 1.B.(6), as part of its support of a proactive approach to mitigating attack vectors, CISA offers several scanning and testing services to assist organizations in reducing their exposure to threats, including vulnerability scanning, web application scanning, phishing campaign assessment, and remote penetration testing.[50] CISA also makes available a wealth of other information and advice on its website. HHS should promote the availability of these services, provided at no cost to critical infrastructure organizations such as hospitals, and encourage all organizations which receive federal funding to avail themselves of CISA's information and advice.

[48] Subcommittee on Privacy, Confidentiality, and Security, "Meeting Summary, Hearing on Security in Healthcare," 5-6, *National Committee on Vital and Health Statistics* (July 14, 2021). https://ncvhs.hhs.gov/wp-content/uploads/2021/11/2021-07-14-NCVHS-PCS-Hearing-Summary-FINAL-508.pdf (Notes on Wong and Kidd testimony).
[49] *Id.*
[50] CISA, "Cyber Hygiene Services," https://www.cisa.gov/cyber-hygiene-services (visited Apr. 11, 2022).

<u>Recommendation 4</u>: Evaluate, in concert with other appropriate government agencies, the level of compliance with the HIPAA Security Rule and provide assistance to healthcare entities with the greatest need in meeting the enhanced minimum security requirements.

Many healthcare organizations — including tribal, public health, state and local governments, and small and medium providers — are challenged by a lack of adequate resources to comply with current and enhanced regulatory requirements. They lack familiarity with available free resources and underestimate risks, and yet it is critical that we raise the level of security compliance and cybersecurity hygiene to better protect the safety of all patients. These resource challenges have been amplified by the pandemic. We recommend that HHS develop incentive programs to support organizations with the greatest need. Providing support to these health organizations would reduce or minimize the impact of cyber-attacks affecting patient safety. For example, though medical device companies may include a "software bill of materials," it is not likely to be cost advantageous for a healthcare system to replace a new device for security reasons unless the device is at the end of its useful life.[51]

One specific challenge that all healthcare organizations share is the upkeep of legacy technology for which basic security controls or patching are no longer supported. Complex health technology is often designed to last many years due to high cost. Unfortunately, many devices including EHRs or other software systems last longer than vendors are willing or able to support them. As a result, these devices lack the latest security features or cannot be patched to correct the latest security vulnerability. For example, studies in 2020 found that "83 percent of medical imaging devices [such as mammography machines, radiology systems, or ultrasounds] run on operating systems that are so old they no longer receive any software updates at all."[52] In the same year, a survey conducted by the Healthcare Information and Management Systems Society, Inc. (HIMSS) found that 80% of respondents had legacy systems in place,[53] a number that is likely unchanged and possibly larger as healthcare organizations have faced financial uncertainty and budget constraints due to the ongoing public health emergency. This means many organizations are using life sustaining devices that can no longer be secured against new cybersecurity threats. Additionally, because these devices can no longer be updated, it also means organizations will be required to maintain auxiliary devices that can pair with those machines, creating an environment of security risks and policy exceptions that could harm a patient were a security gap to be exploited. Hospitals can even crash old devices doing routine security scans if proper precautions are not taken due to interoperability issues that make them "brittle." [54] In some cases, they might not be

[51] A software bill of materials is a formal record containing a "list of ingredients that make up software components," including information about the identity of the suppliers of different components and patch status. It contributes to greater transparency in the software development and acquisition process, increasing cost efficiency as well as mitigating risks in security, licensing, and compliance. See "Software Bill of Materials," *National Telecommunications and Information Administration*. https://ntia.gov/SBOM (visited Apr. 1, 2022).
[52] Lily Hay Newman, "Most medical imaging devices run outdated operating systems," *Wired* (Mar. 10, 2020). https://www.wired.com/story/most-medical-imaging-devices-run-outdated-operating-systems/ (visited Apr. 11, 2022).
[53] "Cybersecurity and Security Incidents in Healthcare Infographic," Healthcare Information and Management Systems Society, Inc. (July 6, 2021). https://www.himss.org/resources/cybersecurity-and-security-incidents-healthcare-infographic (visited Apr. 11, 2022).
[54] The crashing of a device during a security scan can happen for several reasons, one of the most common being that older or legacy devices are not designed for or capable of accommodating the types of information being sent over the network during the scan and respond by failing or shutting down since they cannot interpret the message, or it overloads the system. Sean Gallagher, "Task force tells Congress health IT security is in critical condition" *Ars*

available for patient care until they can be reprogrammed and brought back online.[55] OCR even dedicated its October 2021 Cyber Newsletter to a discussion of how to manage the risks of legacy technologies,[56] but the guidance mostly identifies workarounds for out-of-date technology that is still in use. Even OCR acknowledges that "[i]deally, all organizations would only use information systems that are fully patched and up to date."[57]

To help healthcare entities move toward this ideal state, adopt minimum enhanced security requirements, and manage the cost of replacing legacy technologies that no longer meet minimum security requirements, HHS and other appropriate government agencies should consider evaluating the level of compliance with the HIPAA Security Rule and assisting entities with the greatest need. NCVHS recommends that HHS consider the adoption of robust incentive programs that would support the ability to implement Recommendations 1 and 2, keeping the technology, and consequently, patients safer. There are several options for how an incentive program could work. For example, it could be modeled after the Centers for Medicare and Medicaid's 'Meaningful Use' program which has both financial support and information sharing elements.[58]

Technica (June 8, 2017) (quoting Joshua Corman, co-founder of the information security non-profit organization I-Am-The-Cavalry and a member of the Health Care Industry Cybersecurity Task Force)visited.

[55] See, e.g., Jay Brogan, "An Antivirus Scan Shut Down a Medical Device in the Middle of Heart Surgery," *Slate* (May 5, 2016) (describing an incident in which a tool called the Merge Hemo, which gathers and evaluates cardiac information about a patient and transfers it to a connected computer, crashed when the computer automatically initiated its hourly malware scan while a patient procedure was in progress). https://slate.com/technology/2016/05/antivirus-scan-shuts-down-merge-hemo-medical-device-during-heart-surgery.html (visited Apr. 12, 2022).

[56] OCR**,** "Fall 2021 Cybersecurity Newsletter: Securing Your Legacy," (Oct. 29, 2021). https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2021/index.html.

[57] *Id*.

[58] Office of the National Coordinator for Health Information Technology, "Medicare and Medicaid EHR Incentive Programs: Meaningful Use Core Objectives that Address Privacy and Security" https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-5.pdf (visited Feb. 2, 2022).